REMARKS

This application has been carefully considered in connection with the Examiner's Office Action dated October 30, 2008. Reconsideration and allowance are respectfully requested in view of the following.

Summary of Rejections

Claims 1-24 were pending at the time of the Office Action.

Claims 16-18 and 22-24 were rejected under 35 USC 112.

Claims 16-18 and 22-24 were rejected under 35 USC 103.

Status of the Claims

Claims 16 and 22 have been amended.

Claims 17, 18, 23, and 24 are in original form.

Claims 1-15 and 19-21 were previously withdrawn.

Summary of Claims Pending

Claims 16-18 and 22-24 are currently pending following this response.

Applicant Initiated Interview

Applicants thank Examiner Cristina Sherr for her time and consideration of the arguments presented in the telephone interview on January 22, 2009. In the interview Applicants noted that the prior art required that passwords be decrypted and then provided to the second password repository. However, the claims of the pending application provide a method in which the new repository may populate its datastore with passwords that have been authenticated by the original repository without need of decrypting the password. A detailed discussion of the differences between the applied art and the claim limitations follows.

In the interest of advancing prosecution, the claims have been amended herein as suggested by Examiner Sherr for clarification purposes.

Response to Rejections

Data migration from a first system to a second system is a difficult and time consuming process. The data being migrated may include user information with one or more encrypted data elements. For example, password data may be encrypted to protect the privacy of a user. These encrypted data elements may not be easily decrypted for a number of reasons, including the unavailability of decryption keys. Therefore, alternative solutions to obtaining encrypted data elements during migration are needed. The pending disclosure teaches systems and methods for data migration from a first system to a second system using intercepted data.

Data migration as described throughout the pending disclosure, including paragraphs [0017]-[0026], and as used herein refers to the process by which data is moved from one proprietary system to another proprietary system. For example, the proprietary system by one vendor may store encrypted data using one proprietary encryption scheme while another vendor may use a different proprietary encryption scheme. The data migration process is not simply the copying of data from one source datastore to a target datastore, but rather includes the gathering of data from a source datastore in a first format, converting some or all of the data in the first format to a second format of the target datastore, and then saving the converted data in the second format on the target datastore. In addition, data migration requires that encrypted data elements of the source datastore, such as encrypted password information, which cannot be easily decrypted by the target datastore, be obtained from the user and added to the target datastore. For example, the target datastore may not have decryption keys for decrypting encrypted data

elements of the source datastore. Obtaining encrypted data elements of the source datastore from the user maintains consistency between the contents of the source datastore and the target datastore. This two step process overcomes many of the prior art limitations and does not require the decryption of the source datastore by the target datastore.

As disclosed in paragraph [0021], intercepting data may refer to the process by which a user sends password data intended for the source datastore and the target datastore intercepts the password data. Accordingly, user password information which is stored as encrypted user password information on the source datastore is obtained without decrypting the encrypted user password information on the source datastore. Unlike packet sniffing, interception includes obtaining the password data, verifying the password data, and storing password data in the target datastore. The user password data is intercepted directly from the user and can be verified using the source database. This verification occurs by having the target datastore send the password data to the source datastore, and the source datastore confirming that the password data is valid. Therefore, the target datastore performs the data interception by acting as an intermediary between a user and the source datastore. As described above, encrypted password data may be captured and provided to the target datastore using the interception process, thereby allowing for user passwords and other encrypted data to be migrated from a first proprietary system to a second proprietary system without having every user re-enter their security information.

Sampson, et al. (U.S. Patent No. 6,490,624, "Sampson") relates to a system that controls access to information resources. A session manager enables a client to securely interact with a plurality of access servers and associated runtime elements using a plurality of sessions. The information resources are stored on protected servers. Access to the protected servers is

controlled by one of the access servers. The session manager determines whether the client is involved in an authenticated session with any access server in the system. If so, the client is permitted to access the resources without logging in to the specific access server that is associated with the protected server. In this way, the client can access multiple resources of multiple protected servers without logging in to each of the access servers that controls each of the protected servers. Sampson does not teach or suggest migrating the source datastore to a target datastore where the datastore comprises user identification data. In fact, Sampson is completely unconcerned with migrating data of any type at all. Sampson is simply concerned with providing a single sign on for a user so that the user doesn't have to log in multiple times to access various information on the system. Such a system is unrelated to migrating authentication data from one datastore to another without requiring a user to re-enroll.

Blakley, III et al. (U.S. Patent No. 5,832,211, "Blakley") relates to a network system server that provides password synchronization between a main datastore and a plurality of secondary datastores so that a user is able to maintain a single, unique password among the plurality of secondary datastores. Blakley uses a password synchronization server to store user names and plain-text passwords securely and to respond to requests from secondary datastores for their retrieval. The passwords are sent to the secondary datastores using encryption that is decipherable by the secondary datastores. Blakley does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information and without decrypting the data stored in the first vendor's product.

Mehring et al. (U.S. Patent No. 6,609,115, "Mehring") relates to a method of allowing a remote system user to request multiple software applications using a single log-in. Although the remote user is only required to log-in once, the user information is submitted to the policy server every time the remote user logs-in to a different web server. Like Blakley, Mehring does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information. It is respectfully submitted that Mehring does not cure the deficiencies of Blakley.

These distinctions, as will other distinctions, will be discussed in more detail in this paper.

Response to Rejections under Section 112

Claims 16-18 and 22-24 were rejected under 35 USC § 112, second paragraph as having insufficient antecedent basis for the limitation in the claims.

Claims 16 and 22 recite the limitation "the source user datastore" and "the corresponding identification." Claim 16 also recites the term "the password." Claims 16 and 22 have been amended to read "the source datastore" and "a corresponding identification." Antecedent basis for the term "the password" recited in line 13 of claim 16 may be found in line 12 of claim 16. Applicants respectfully request the rejection to claims 16 and 22 under 35 USC § 112 second paragraph be withdrawn.

Claims 17, 18, 23 and 24 depend directly or indirectly from independent claims 16 and 22, respectively. Applicants respectfully request the rejection to dependent claim 17, 18, 23 and 24 under 35 USC § 112 second paragraph be withdrawn.

Response to Rejections under Section 103

Claim 16:

Claim 16 was rejected under 35 USC § 103(a) as being unpatentable over Sampson et al, U.S. Patent No. 6,429,624 ("Sampson") in view of Blakley, III et al, U.S. Patent No. 5,832,211 ("Blakley").

I. Blakley does not teach or suggest capturing the password provided to the source user authenticator, monitoring the source user authenticator for an approval response and populating the target datastore with the captured password upon receipt of an approval response.

Claim 16 of the pending application recites in part:

> capturing the password provided to the source user authenticator by the user in response to prompting by the source authenticator,
> monitoring the source user authenticator for an approval response,
> populating the target datastore with the captured password upon receipt by the target datastore of an approval response from the source user authenticator.

Thus, migrating password data from a source (or first) datastore to a target (or second) datastore according to the method of claim 16 may be accomplished without decrypting the password data stored in the source datastore and copying the decrypted password data to the target datastore. Rather, the interceptor captures the password provided by the user to the source user authenticator in response to prompting by the source user authenticator and waits to see whether the source user authenticator approves the user. If the source user authenticator approves the

user's password, then the target user authenticator can populate its own datastore with the captured password knowing that the captured password is authentic. In some cases, the password data may be stored in the source datastore as, for example, a hash or other format that is not subject to being decrypted. However, such a method of storage is no impediment for migrating password data from the source datastore to the target datastore according to the method of claim 16 since no decryption is necessary. The only requirement is that the source user authenticator is still functioning such that it is able to verify that the entered password is authentic.

The Office Action dated October 30, 2008, acknowledges that Sampson does not teach these elements of claim 16 recited above, but alleges that Blakley does disclose these elements. Applicant respectfully disagrees. In contrast to claim 16, Blakley requires that passwords stored in a first datastore be decrypted and then passed as plain text passwords to the second datastore. See, for example, Blakley, column 8 which states that "if the value is identified, the password synchronization server retrieves client W's password from the password repository and decrypts it. Next, in block **450**, the password synchronization server returns client W's password to foreign registry Z." This is a completely different method for transferring password data from one repository to another and is inapplicable to systems in which the password is stored as, for example, a hash, which is an item typically not capable of being decrypted.

II. Neither Sampson nor Blakley teach or suggest migrating password data from a source datastore to a target datastore.

Claim 16 of the pending application recites "migrating the source datastore to the target datastore, wherein the source datastore comprises user identification data and user authentication data." The Office Action alleges that Sampson discloses this feature citing various passages in

columns 6, 7, and 17. Applicants respectfully disagree with this assertion. Sampson relates to a system that controls access to information resources. (See, Sampson, Abstract). Sampson discloses a session manager that determines whether the client is involved in an authenticated session with any access server in the system. If so, the client is permitted to access the resources without logging in to the specific access server that is associated with the protected server. Thus, Sampson merely teaches a single sign on system such that a user only has to authenticate themselves once rather than multiple times even though the system may include multiple protected resources requiring authentication. Sampson does not disclose migrating identification and authentication (e.g., password) data from a source datastore to a target datastore. In fact, Sampson is completely unconcerned with migrating data of any type at all. Sampson is simply concerned with providing a single sign on for a user so that the user does not have to log in multiple times to access various information on the system. Such a system is unrelated to migrating authentication data from one datastore to another without requiring a user to re-enroll.

Blakley does not cure this deficiency in Sampson. Blakley provides password synchronization between a main data store and a plurality of secondary data stores. (See, for example, Blakley, Abstract). This enables the user to maintain a single, unique password among the plurality of secondary datastores. This is similar to the teachings of Sampson. Thus, Blakley uses a password synchronization server to store user names and plain-text passwords securely and to respond to requests from secondary datastores for their retrieval. The passwords are sent to the secondary datastores using encryption that is decipherable by the secondary datastores. However, notably absent from Blakley is any teaching or suggestion of migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one

vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information and without decrypting the data stored in the first vendor's product.

For at least the reasons established in sections I and II, Applicants respectfully submit that independent claim 16 is not taught or suggest by Sampson in view of Blakley and respectfully request allowance of this claim.

Claims Depending from Claim 16:

Claims 17-18 were rejected under 35 USC § 103(a) as being unpatentable over Sampson in view of Blakley further in view of Mehring et al., U.S. Patent No. 6,609,115 ("Mehring").

Dependent claims 17 and 18 depend directly or indirectly from independent claim 16 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I and II above, Applicants respectfully submit that dependent claims 17 and 18 are not taught or suggested by Sampson in view of Blakley and respectfully request allowance of these claims. Mehring does not cure the deficiencies of Sampson in view of Blakley.

Claim 22:

Claim 22 was rejected under 35 USC § 103(a) as being unpatentable over Sampson in view of Blakley.

Claim 22 includes limitations substantially similar to the limitations discussed in sections I and II above. For example, claim 22 includes the limitation of:

> using the source user authenticator to prompt for and receive the identification and a password from the user, the target user authenticator: monitors the source user authenticator for an approval response, and upon an approval response from the source user authenticator, captures the password provided to the source user authenticator by the user in response to prompting by the source authenticator, populates the target datastore with the captured password, and associates the captured password with the corresponding identification.

Claim 22 also includes the limitation of "migrating the source datastore to the target datastore, wherein the source datastore comprises user identification data and user authentication data, wherein the source datastore is associated with a source user authenticator, wherein the target datastore is associated with a target user authenticator, and wherein the target user authenticator is in communication with the source user authenticator." Accordingly, the arguments of sections I and II are hereby repeated for claim 22.

For at least the reasons established in sections I and II, Applicants respectfully submit that independent claim 22 is not taught or suggest by Sampson in view of Blakley and respectfully request allowance of this claim.

Claims Depending from Claim 22:

Claims 23-24 were rejected under 35 USC § 103(a) as being unpatentable over Sampson in view of Blakley further in view of Mehring.

Dependent claims 23 and 24 depend directly or indirectly from independent claim 22 and incorporate all of the limitations thereof. Accordingly, for at least the reasons established in sections I and II above, Applicants respectfully submit that dependent claims 23 and 24 are not taught or suggested by Sampson in view of Blakley and respectfully request allowance of these claims. Mehring does not cure the deficiencies of Sampson in view of Blakley.

Conclusion

Consideration of the foregoing amendments and remarks and reconsideration of the application is respectfully requested by Applicants. No new matter is introduced by way of this response. If any fee is due as a result of the filing of this paper, please appropriately charge such fee to Deposit Account Number 21-0765 of Sprint. If a petition for extension of time is necessary in order for this paper to be deemed timely filed, please consider this a petition therefore.

If a telephone conference would facilitate the resolution of any issue or expedite the prosecution of the application, the Examiner is invited to contact the undersigned at the telephone number given below.

Respectfully submitted,

Date: January 30, 2009

/Michael W. Piper/
Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANTS

CONLEY ROSE, P.C.
5601 Granite Parkway, Suite 750
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)